

115TH CONGRESS  
2D SESSION

# H. R. 5433

To require the Secretary of State to design and establish a Vulnerability Disclosure Program (VDP) to improve Department of State cybersecurity and a bug bounty program to identify and report vulnerabilities of internet-facing information technology of the Department of State, and for other purposes.

---

## IN THE HOUSE OF REPRESENTATIVES

APRIL 5, 2018

Mr. TED LIEU of California (for himself and Mr. YOHO) introduced the following bill; which was referred to the Committee on Foreign Affairs

---

## A BILL

To require the Secretary of State to design and establish a Vulnerability Disclosure Program (VDP) to improve Department of State cybersecurity and a bug bounty program to identify and report vulnerabilities of internet-facing information technology of the Department of State, and for other purposes.

1       *Be it enacted by the Senate and House of Representa-*  
2       *tives of the United States of America in Congress assembled,*

3       **SECTION 1. SHORT TITLE.**

4       This Act may be cited as the “Hack Your State De-  
5       partment Act”.

1   **SEC. 2. DEFINITIONS.**

2       In this Act:

3           (1) DEPARTMENT.—The term “Department”  
4       means the Department of State.

5           (2) INFORMATION TECHNOLOGY.—The term  
6       “information technology” has the meaning given  
7       such term in section 11101 of title 40, United  
8       States Code.

9           (3) SECRETARY.—The term “Secretary” means  
10       the Secretary of State.

11   **SEC. 3. DEPARTMENT OF STATE VULNERABILITY DISCLOSURE PROGRAM.**

13       (a) IN GENERAL.—Not later than 180 days after the  
14       date of the enactment of this Act, the Secretary shall de-  
15       sign, establish, and make publicly known a Vulnerability  
16       Disclosure Program (VDP) to improve Department cyber-  
17       security by—

18           (1) providing security researchers with clear  
19       guidelines for—

20                  (A) conducting vulnerability discovery ac-  
21                  tivities directed at Department information  
22                  technology; and

23                  (B) submitting discovered security  
24       vulnerabilities to the Department; and

(2) creating Department procedures and infrastructure to receive and fix discovered vulnerabilities.

4       (b) REQUIREMENTS.—In establishing the VDP pur-  
5 suant to paragraph (1), the Secretary shall—

(1) identify which Department information technology should be included in the program;

8                   (2) determine whether the program should dif-  
9                   ferentiate among and specify the types of security  
10                  vulnerabilities that may be targeted;

1                         (6) consult with the relevant offices at the De-  
2 partment of Defense that were responsible for  
3 launching the 2016 Vulnerability Disclosure Pro-  
4 gram, “Hack the Pentagon”, and subsequent De-  
5 partment of Defense bug bounty programs;

6                         (7) engage qualified interested persons, includ-  
7 ing nongovernmental sector representatives, about  
8 the structure of the program as constructive and to  
9 the extent practicable; and

10                         (8) award a contract to an entity, as necessary,  
11 to manage the program and implement the remedi-  
12 ation of discovered security vulnerabilities.

13                         (c) ANNUAL REPORTS.—Not later than 180 days  
14 after the establishment of the VDP under subsection (a)  
15 and annually thereafter for the next six years, the Sec-  
16 retary of State shall submit to the Committee on Foreign  
17 Affairs of the House of Representatives and the Com-  
18 mittee on Foreign Relations of the Senate a report on the  
19 following with respect to the VDP:

20                         (1) The number and severity, in accordance  
21 with the National Vulnerabilities Database of the  
22 National Institute of Standards and Technology, of  
23 security vulnerabilities reported.

24                         (2) The number of previously unidentified secu-  
25 rity vulnerabilities remediated as a result.

(3) The current number of outstanding previously unidentified security vulnerabilities and Department of State remediation plans.

(4) The average length of time between the reporting of security vulnerabilities and remediation of such vulnerabilities.

7                   (5) An estimate of the total cost savings of dis-  
8                  covering and addressing security vulnerabilities sub-  
9                  mitted through the VDP.

10                         (6) The resources, surge staffing, roles, and re-  
11                         sponsibilities within the Department used to imple-  
12                         ment the VDP and complete security vulnerability  
13                         remediation.

16 SEC. 4. DEPARTMENT OF STATE BUG BOUNTY PILOT PRO-  
17 GRAM.

18 (a) ESTABLISHMENT OF PILOT PROGRAM.—

1                             (2) REQUIREMENTS.—In establishing the pilot  
2                             program described in paragraph (1), the Secretary  
3                             shall—

4                                 (A) provide compensation for reports of  
5                             previously unidentified security vulnerabilities  
6                             within the websites, applications, and other  
7                             internet-facing information technology of the  
8                             Department that are accessible to the public;

9                                 (B) award a contract to an entity, as nec-  
10                             essary, to manage such pilot program and for  
11                             executing the remediation of security  
12                             vulnerabilities identified pursuant to subpara-  
13                             graph (A);

14                                 (C) identify which Department information  
15                             technology should be included in such pilot pro-  
16                             gram;

17                                 (D) consult with the Attorney General on  
18                             how to ensure that approved individuals, orga-  
19                             nizations, or companies that comply with the  
20                             requirements of such pilot program are pro-  
21                             tected from prosecution under section 1030 of  
22                             title 18, United States Code, and similar provi-  
23                             sions of law for specific activities authorized  
24                             under such pilot program;

1                         (E) consult with the relevant offices at the  
2                         Department of Defense that were responsible  
3                         for launching the 2016 “Hack the Pentagon”  
4                         pilot program and subsequent Department of  
5                         Defense bug bounty programs;

6                         (F) develop a process by which an ap-  
7                         proved individual, organization, or company can  
8                         register with the entity referred to in subparagraph  
9                         (B), submit to a background check as de-  
10                        termined by the Department, and receive a de-  
11                        termination as to eligibility for participation in  
12                        such pilot program; and

13                        (G) engage qualified interested persons, in-  
14                        cluding nongovernmental sector representatives,  
15                        about the structure of such pilot program as  
16                        constructive and to the extent practicable.

17                        (b) REPORT.—Not later than 90 days after the date  
18                        on which the bug bounty pilot program under subsection  
19                        (a) is completed, the Secretary shall submit to the Com-  
20                        mittee on Foreign Relations of the Senate and the Com-  
21                        mittee on Foreign Affairs of the House of Representatives  
22                        a report on such pilot program, including information re-  
23                        lating to—

24                        (1) the number of approved individuals, organi-  
25                        zations, or companies involved in such pilot pro-

1       gram, broken down by the number of approved indi-  
2       viduals, organizations, or companies that—  
3                   (A) registered;  
4                   (B) were approved;  
5                   (C) submitted security vulnerabilities; and  
6                   (D) received compensation;

7                   (2) the number and severity, in accordance with  
8       the National Vulnerabilities Database of the Na-  
9       tional Institute of Standards and Technology, of se-  
10      curity vulnerabilities reported as part of such pilot  
11      program;

12                  (3) the number of previously unidentified secu-  
13      rity vulnerabilities remediated as a result of such  
14      pilot program;

15                  (4) the current number of outstanding pre-  
16      viously unidentified security vulnerabilities and De-  
17      partment remediation plans;

18                  (5) the average length of time between the re-  
19      porting of security vulnerabilities and remediation of  
20      such vulnerabilities;

21                  (6) the types of compensation provided under  
22      such pilot program; and

23                  (7) the lessons learned from such pilot pro-  
24      gram.

